USAWC STRATEGY RESEARCH PROJECT

OUR NATIONAL INFORMATION INFRASTRUCTURE; AN IMMEDIATE STRATEGIC CONCERN IN NATIONAL SECURITY POLICY

by

Lieutenant Colonel Brian P. Hamilton
United States Army

William Waddell
Project Advisor

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 MAY 2004		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Our National Information Infrastructure An Immediate Concern in National Security Policy	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Brian Hamilton	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**24**	

ABSTRACT

AUTHOR: LTC Brian P. Hamilton

TITLE: Our National Information Infrastructure; An Immediate Concern In National Security Policy

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 24 CLASSIFICATION: Unclassified

The United States continues to experience a phenomenal growth in the Internet combined with an increased dependence upon the automated systems within its information infrastructure. This tremendous growth is accompanied with a commensurate increase in cyber attack and crime. Both nonstate and state sponsored enemies are becoming more organized and talented, and experts view the greatest dangers in cyberspace as villains lying in wait, withholding full-fledged cyber attack until the opportunity for sufficient strategic advantage presents itself. The United States' current security policies and strategies depend upon voluntary adherence to government recommendations with few regulations, standards or financial incentives to gain private sector support. The potential losses associated with failing to secure cyberspace are too high. This paper provides an assessment of national efforts to secure cyberspace and puts forward recommendations to strengthen this critical national infrastructure. The United States must reassess its national strategies and with practical incentives, enforce stronger measures to secure its information infrastructures. Otherwise, the nation will face unforeseen, potentially catastrophic consequences.

TABLE OF CONTENTS

OUR NATIONAL INFORMATION INFRASTRUCTURE; AN IMMEDIATE STRATEGIC CONCERN IN NATIONAL SECURITY POLICY

> In the past few years, threats to cyberspace have risen dramatically. The policy of the United States is to protect against debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States.
>
> President George W. Bush[1]

INTRODUCTION

Technology advances of the information age have created an unimaginable boom in computing and a tremendous growth in the networks that support these processes. Countless national systems, both in civilian and government sectors, depend upon the Internet for transfer of information, including email, e-commerce, database management and telemetry. In its 1997 "Report to the President's Commission on Critical Infrastructure Protection", the Software Engineering Institute of Carnegie Mellon University described the integration of computers into American business and government to the extent that "computer-related risks cannot be separated from general business, health and privacy risks".[2] Updating the magnitude of this report, the Internet Software Consortium estimates the number of users on the Internet in 2003 as 171,638,297, over tenfold growth from 16,146,000 users at the time of the 1997 Carnegie Mellon publication.[3] Clearly, the protection of our national information infrastructure presents a vital interest to our national security and this critical national asset depends implicitly upon the rapidly expanding, increasingly complex Internet. This report serves to examine the threat against our critical infrastructure and our national actions to mitigate our risks in cyberspace.

BACKGROUND

While arguably one of the prime enablers of the information age, the Internet also presents the greatest vulnerability to the protection of our national information infrastructure. The expansive Internet provides both tools and sanctuary for information system attackers and intruders (for this report collectively termed "hackers"). From the would-be hacker with little computer knowledge to state-sponsored cyber attack organizations, the Internet provides the medium to exchange illicit software and knowledge on information attack. Also, with the

connectivity of the Internet crossing geographic boundaries, hackers and hacker organizations find refuge from detection and protection from prosecution in the gray area of international and domestic laws. In illustration of this digital sanctuary, an amateur hacker caused direct economic damage to a country over 5000 miles away and when finally discovered, he escaped prosecution. In this case, Israel suffered a national loss of $12 million due to the globally distributed "Love" virus, yet it could not file charges against the originator as his home country, the Philippines, did not make virus writing illegal until after the event.[4] This case illustrates the sanctuary of the Internet as well as the pace at which technology has outpaced governments and legal systems. The same attributes that enhanced the Internet's original purpose of information exchange between academics and government research agencies have provided a rich breeding ground for information attack.

THE THREAT FROM OUTSIDE THE WALLS

In 1997, the President's Commission on Critical Infrastructure Protection (PCCIP) illustrated the prime vulnerabilities of the Internet as denial of service attacks, spoofing and sniffers.

- ***Denial of service*** attacks overload an Internet site with synchronization requests and thus render the target system inoperative and, in the case of an Internet Service Provider (ISP), denies information service to all connected users.
- ***Spoofing*** is misrepresenting one's attacking system as a trusted user, either through email or interactive session, to gain sensitive information or illegal system use.
- ***Sniffers*** monitor traffic at key points within the unsecured, ubiquitous Internet and illicitly retrieve unlawful data such as sensitive information, user ID's and passwords.

These attacks were not deemed as theoretical, but were derived from actual attacks reported to the Computer Emergency Reaction Team (CERT) Coordination Center.[5]

One area this early report overlooked was the Internet phenomena of viruses. ***Viruses*** are malicious code hidden within a seemingly innocent program, normally attached as an email enclosure. Once an unsuspecting victim executes the virus code, it normally distributes itself to other potential target systems (via email attachment) and oftentimes, proceeds to destroy stored data on its current host. The effect of this type of virus is to inflict damage on the user's systems and of larger impact, congest the Internet and Internet servers with spurious emails. More dangerous virus variants remain hidden within the users' system awaiting directions via

the Internet to perform malicious functions (known as ***Zombies***) or silently report sensitive information, such as passwords and bank accounts, to distant Internet servers (known as ***Spyware***). Hackers also manually plant zombies and spyware in systems that are not properly secured against Internet intrusion.

Although not addressed by the 1997 Carnegie Mellon report, the largest potential for immediate, broad scale cyber attack damage to the United States lies in the ability to hijack specialized digital devices that serve as the brains of critical industry and government operations. These devices, called ***Distributed Control Systems*** (DCS) and ***Supervisory Control and Data Acquisition*** (SCADA) nodes, perform a wide variety of remotely attended tasks such as switching electricity within power grids, throwing railway switches, reconfiguring communications networks and operating valves in pipelines that carry oil, gas and water. These devices, if controlled by our enemies, could impact all aspects of national life through countless means including shutting down power girds, stopping air and rail traffic and clogging communications networks.

When corrupted, DCS and SCADA devices can produce unimaginable results, as was the case in Queensland, Australia in early 2000. Vitek Boden, a disgruntled ex-employee of a telemetry equipment supplier, commandeered over 300 SCADA nodes belonging to the Maroochy Shire, Queenland wastewater system. Using a stolen laptop computer and radio, Boden dumped hundreds of thousands of gallons of putrid waste into his surrounding community, killing marine life, contaminating rivers, and disrupting life and business with an "unbearable" stench. Although it was his 46th successful intrusion, Boden was arrested only when police came upon his suspicious vehicle parked alongside the roadway. By remote control from his pirate command center, he "could have done anything he liked to the fresh water" according to Paul Chisholm, Chief Executive Officer, Hunter Watertech, supplier of telemetry devices.[6]

Boden's intent was to gain a consulting job with Maroochy Shire and solve their "problem" of leaking wastewater. He established criminal control over the 300 SCADA nodes to harass the utility service for his economic gain. With his sporadic attacks, he damaged the ecology and hindered business, particularly the local Hyatt Regency hotel. It is important to realize Boden's damage was limited by his objective. He did not desire to destroy the community, but to manipulate their business decisions. If Boden had been a terrorist, he could have caused tremendous environmental and economic damage to Maroochy Shire, whose 118,000 residents depend upon 700,000 tourists to bring $300 million (Australian) to their portion of Australia's Sunshine Coast.[7] If he had been a terrorist hijacking SCADA nodes of a major US city, the

results could have easily translated into a national emergency of containing the environmental impact, providing fresh water, and controlling disease.

The value of DCS and SCADA nodes has not gone unnoticed by our adversaries. Due to recent discoveries, the threat capability normally attributed to state-sponsored cyber attack organizations, such as China and Russia, is now being expanded to terrorists. Recently in Afghanistan, US forces found Al Qaeda laptops with evidence of research of digital switches that control utilities, system cracking tools, scanners for security flaws and computer models of a dam. More startling, they found software used in predicting "the course of a wall of water surging downstream". Member of the President's Commission on Critical Infrastructure Protection and US intelligence agencies agree that we have underestimated terrorist's interest in cyber attack, yet they view these attacks as a means to amplify the consequence of direct kinetic attacks.[8]

THE THREAT FROM WITHIN

The threat discussed thus far has been focused upon external intruders attacking our information systems. While this is a formidable threat, it is inevitable that we will experience an attack from commercial software purchased and installed by ourselves. Today's sophisticated commercial computer programs require millions of lines of source code and serve as a lucrative hiding place for Trojan Horse routines. A ***Trojan Horse*** is a malicious program hidden within a legitimate application that can perform any of the variety of hacker threats discussed earlier. Once installed on a computer, the system considers it trusted and allows the infected program to execute its instructions. It is important to realize that this malicious programming can impact the software function of traditional computing as well as the firmware that controls the workhorse computers found in automobiles, aircraft, railroad engines, microwave ovens, weapon systems and thousands of other automated systems found in every day life. The Trojan Horse can activate based upon a date or series of events within the computer system. More flexible and attractive to the hacker, the Trojan Horse can serve as a zombie awaiting distant commands, as a backdoor to control the system via the Internet or as spyware, reporting the system's sensitive information.

The likelihood of Trojan Horse routines existing within commercial software is extremely high. Very few software companies require background investigations on information technology (IT) personnel and at most, they perform background checks by reviewing references. As risky as this may seem, the latest trend of offshore outsourcing of software development exponentially increases the threat and raises the issue of a trend that places our

national information infrastructure at risk. At the 2003 Techno-Security Conference, users questioned the wisdom of offshore software development by corporations aiming to reap the benefits of cheap labor. The level of risk and outcome of this risky venture is criticized as unknown. Although an unevaluated danger, the threat is clearly present, especially when the work is going to countries such as China with its extensive technology espionage networks and countries in Southeast Asia where terrorist networks are known to exist.[9]

Fortune 500 companies have embraced the concept of offshore software development with heavy investments. For example, Adobe spent $50 mil in 2001 to expand its programming and research center in New Delhi, India.[10] The reason is simple; lower labor costs. To highlight our Adobe example, the starting salary of a software engineer in India is $5000; while experienced engineers receive $10000 and top IT professionals earn approximately $20,000. Meanwhile, US IT jobs are down 20% since 2000 and senior software engineer salaries have fallen from $130,000 to $100,000.[11] Business is shifting its production of software overseas and views this change as a survival effort in a tough global IT market.

While the move to overseas outsourcing has been accelerated, business has been slow to ensure their software remains trustworthy. Companies investing in offshore software development must emplace verification and auditing systems, yet according to Tim McKnight, Chief Information Assurance Officer at Northrup Grumman, this will be costly. Citing his experience at Cisco Systems, he stated the corporation would send teams overseas to monitor file and source code servers and perform risk assessments. Yet through all the efforts, he claimed it was "very difficult to know who these people are. It can be done, [but] you really need buy-in from the top of the corporation."[12] In Japan, this international trend is focused upon China with Japanese blue chip corporation investments pushing China from the "factory to the world" to the "design laboratory of the world". This effort focuses on both software engineering and chip production.[13] The trend for offshore software development, with its inherent risk to our national information infrastructure, is an increasing international business trend, yet the means to perform auditing and verification is almost nonexistent.

THE HIDDEN WAR

In recent years, the vulnerabilities of the Internet have translated into an alarming number of attacks on our national information infrastructure. To illustrate, the nation's power grid is one critical area under cyber attack. Since the widespread acceptance of the Internet, power companies have embraced the advantage of remote operation, via SCADA/DCS nodes, of equipment spread over large distances. In the spring of 2001, unknown hackers penetrated and

gained control of systems within California Independent System Operator (Cal-ISO), the state manager of long distance electricity transmission. Fortunately, the attacked computer systems were confined to a practice network disconnected from the power grid that controls much of the Western US, yet it served as the first publicly acknowledged cyber attack to gain control of part of our national infrastructure.[14] The alarming point of this 17-day intrusion into California's electricity control systems is that it appears the hackers were of Chinese origin, linked to the Honkers Union of China (HUC). "Honker" is the Chinese derivative of the work hacker. During the same period of the intrusion, HUC defaced CAL-ISO websites with Chinese flags, statements decrying US imperialism and pictures of the Wang Wei, the Chinese F-8 fighter pilot who collided with a US spy plane on April 1st, 2001. Yet, as is often the case in computer attack, it is extremely difficult to conclusively identify the assailants.[15]

Many of the attacks on our systems appear to be well organized and well concealed. In the six months following the World Trade Center attack, security companies logged 129,000 intrusions targeted against the nation's power grid, many of which appeared to be sponsored by governments or organizations in the Middle East.[16] Last year, U.S. intelligence officials discovered an Al Qaeda safe house in Pakistan devoted to training hacker skills and cyber warfare, termed a "cyber academy". During the same period, 60 percent of power and energy companies experienced at least one severe cyber attack during the last half of 2002.[17] These cyber attacks are difficult to assess as corporations are hesitant to admit that they have been successfully attacked. With good fortune, none of these attacks proved catastrophic, yet the events clearly illustrate the ongoing, hidden war in cyberspace and the potential for greater exploitation of our information infrastructure vulnerabilities.

The soldiers in this hidden war fall into several different categories. First, there are misguided thrill seekers, termed as **hackers**, **crackers** and **phreakers** to name a few, who intrude upon or disrupt information systems to gain internal satisfaction or external recognition from their peers. Using a Western analogy of good and bad, they usually split into two subcategories, "**white hat**" and "**black hat**" hackers, and can also qualify as "hacktivists" or criminals, as discussed below. Second, there is the **criminal element** whose intent is illicit gain through identity theft, mail fraud and other crimes. Third, there are politically or nationally inspired activists, sometimes termed **hactivists**, that attack information systems for ideological reasons. An example of this is the Palestinian-Israeli cyber war of 2000. This series of cyber attacks started with simple web site defacements and then quickly escalated into a "cyber jihad" with a large number of denial of service attacks, which slowed the Middle East's sparse Internet infrastructure and damaged E-business.[18] While at first glance, one might think the cyber

combatants were confined to Palestine or Israel, yet with a zeal of volunteerism based upon political ideals, volunteers from around the world joined the fight. This made the Palestinian-Israeli cyber war a world war that caused damage to computer systems across many national boundaries. Fourth, there are **nonstate sponsored hackers**, previously discussed in this report as terrorists. As another example of nonstate sponsored actors, Zapatista guerillas used the Internet to disseminate their revolutionary views and effectively jam Mexican government web sites.[19] In the case of terrorists, it is commonly believed within the cyber security community that full scale, nonstate sponsored cyber attack will be used to amplify kinetic strikes. Finally and potentially most dangerous, **state sponsored cyber attack organizations** are growing in strength. Many nations, including the US, have developed their own ability to conduct network attack. As early as 1999, the Chinese Liberation Army Daily published that integrating network warfare with warfare on the ground was essential to winning future conflicts.[20] While many believe governments may have secretly supported hacktivists, state sponsored cyber attack has not been reported and confirmed to date. This is due to the secrecy surrounding these activities and more importantly, because governments withhold their full network attack capability to achieve surprise at the proper strategic moment. Up to now, there has not been an event to warrant unbridled network attack.

THE RESPONSE

The United States has been slow to react to the threat described by the 1997 Carnegie Mellon report. After reviewing this report, the President's Commission on Critical Infrastructure Protection issued a report in October 1997, calling for "a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures".[21] On 22 May 1998, President Clinton announced Presidential Decision Directive (PDD) 63, which focused upon physical and cyber attack.[22] PDD 63 set a goal of "reliable, interconnected, and secure infrastructure by the year 2003 and significantly increased security for government information systems by the year 2000". More challenging, it set a deadline of 2003 to build the capability to protect critical infrastructures from intentional act.[23] While PDD 63 may have experienced some success within the government sector, it has failed to meet its private sector goals as the strategy alone, The National Strategy to Secure Cyberspace, was not published until February 2003.[24]

The National Strategy to Secure Cyberspace serves as the nation's plan to secure our critical information infrastructures, yet this strategy has received tremendous criticism to the extent of being termed "useless".[25] The main criticism of the strategy is that it lacks any means

of enforcement or standardization. The strategy emphasizes recommendations for improving security and partnering between government, the private sector and citizens, yet it does not set standards or emplace federal regulations to protect the Internet. The administration backed away from original regulations, such as requiring free security software with home Internet service and restricting the use of vulnerable wireless networks. Critics have charged that these initiatives were dropped as a result of lobbying from technology firms, which desired to avoid "potentially costly government restrictions".[26] Finally, the strategy offers no incentives for the private sector to incur the cost of Internet security. Strategy critics strongly argue that to convince industry to secure its networks, the government should offer tax and other financial incentives.[27] The strategy falls short of protecting cyberspace by relying upon users to exercise more responsibility on the Internet and the voluntary adoption of costly security measures.

A review of the National Strategy to Secure Cyberspace reveals varying levels of strategy for different segments of our society. At the federal level, the document outlines security improvements to the US government information infrastructure that are tied to budget, delegated to action agencies, assessed by "red teams" and periodically reviewed by committee. Also, clarifying previous positions, the document states that the US response to cyber attack will not be limited to criminal prosecution, but that the US will respond in an "appropriate manner." At the state and local government level, the wording becomes less direct and focuses upon awareness training and encouragement to develop IT security. Finally, when discussing business and individual users, the strategy emphasizes information sharing, coordination and encouragement of the private sector to secure our information infrastructure.[28] When examining the direction for the three major groups within the strategy, the document provides fairly clear direction for the federal government to defend its critical infrastructure while almost leaving state/local governments and business/public users to solve the security of cyberspace on their own. For this reason, the plan falls short of a national strategy.

In 1998 with the publication of PDD 63, the United States formally recognized the critical need for securing the vulnerabilities of cyberspace yet its actions in overall security policy have not matched the priority of protecting this vital resource. Condeleezza Rice, the National Security Advisor has stated that the protection of critical infrastructures is a priority national security objective. Yet at the same time, the latest US National Security Strategy (NSS) is seen as "devoid of any information infrastructure issues"[29] and the National Strategy to Secure Cyberspace falls far short of providing protection of our critical information assets. Our nation's security policy must recognize that the Internet, with its global networks and millions of

computer systems, is a 21st Century battle space that directly threatens our critical information infrastructures in order to achieve the priority necessary to combat this looming threat.

The response of the United States to the demonstrated dangers to our national information infrastructure has been one of moderately proactive measures at the federal level and passive measures elsewhere. For state and local governments, as well as the general public and business, the national strategy encourages action and promotes the federal government as an example for others to follow. This mainly passive approach however seems to apply a *laissez faire* methodology to the critical task of protecting our national information infrastructure. Applying a business principle to a national security issue, the defense of our information systems warrants more direct action and must be a unified, cross-sector approach for several reasons. First, whether public or private, our computer systems share the same Internet for the transfer of data. It does not matter if your local area networks are free from attack if the connecting Internet is disabled or your servers are bombarded with emails from infected systems. Secondly, a determined adversary will exercise an asymmetric approach to attacking the US. For example, if federal agencies are strong in cyber defense, our adversaries will attack the portion of national infrastructure that is susceptible to their threat. In the end, all sectors of the national information infrastructure lose in a catastrophic attack. Finally, when faced with costly information security measures, companies and individuals have demonstrated a lax attitude towards expending resources to ensure the trustworthiness and reliability of their information systems. The Gartner Group predicts that 90% of cyber attacks through 2005 will occur by exploiting known security flaws for which there are known preventive measures. This vulnerability is due to vendors delivering systems with security features disabled, a lack of qualified IT security personnel and a lack of specificity of information security standards.[30] When faced with expenditures to improve operations or improve security, management has chosen operations where the benefits are more readily understood and achieved. The National Strategy to Secure Cyberspace must take more active measures to protect the entire information infrastructure of the United States.

THE WAY AHEAD

When examining the issue of securing the nation's information infrastructure, there is a balance of control extending from draconian government regulation to totally unregulated activity. The current strategy proactively guides the activities of the federal government while, although not totally unregulated, allows other sectors of the information infrastructure to determine their levels of security based upon self-interest, individual responsibility and

organizational needs. Cumbersome and disjointed, this strategy will prove difficult to achieve the goal of infrastructure protection since the national information infrastructure is only as strong as the sum of its components and the competitive private sector has proven itself slow in correcting its vulnerabilities. Due to the nature of the Internet and information systems, the actions or inactions of any sector can adversely impact other members of the network. Therefore, the national strategy must be strengthened and provide clearer direction to protect our infrastructure from adversary attack.

Richard Clarke, former Cyber Security Director, countered critics of the newly published National Strategy for Securing Cyberspace by arguing that cyber security is so complex that it defies a centralized, regulatory approach.[31] While this may be true, there are strategies that provide dynamic means to strengthen the nation's information infrastructure in a more balanced manner. Combined with awareness of the threat, private and government sectors will respond to forward-looking laws, incentives and realistic appraisals of their information defense capabilities. By increasing the clarity and appeal of the current strategy, the US can preserve its information infrastructure to support the nation in times of peace and crisis.

The national strategy must reexamine the nation's laws concerning cyber security. First, manufacturers and vendors must realize liability for the trustworthiness of their systems and software. Whether produced domestically or by offshore outsourcing, manufacturers must emplace reasonable verification, validation and standards for safeguarding software from security flaws. Therefore, the Department of Homeland Security, through the President's Commission on Critical Infrastructure Protection, should lead a consortium of government and private sector members to establish reasonable practices for production of IT components. With a foundation of production standards of trustworthiness, manufacturers would then be liable for failure to ensure IT integrity. Second, the nation must update its laws to match the severity of damage related to hacker activity. When four viruses can cost the nation $12 billion and one virus alone can shut down 350,000 servers [32], hackers can no longer be viewed as harmless, misdirected nonconformists. Their actions are deliberate, premeditated and they must be prosecuted in the manner commensurate to that of a federal felon or terrorist. Finally, the US must continue its efforts to update international law to match the modern challenges of cyber security.

The federal government should provide incentives to private and government sectors to promptly upgrade their cyberspace security. For business, the US government should provide tax incentives for procurement of security measures and the production of security-conscious technology. Currently, business views IT expenditures as competition for operational resources.

Along with awareness, carefully crafted tax incentives can stimulate business to emplace cyberspace security measures and produce attack resistant information technology. With liability for failure and incentives for success, security investments can successfully compete in the boardrooms of corporate America. For individuals, the government implemented a limited program of "cybercops" or scholarships for IT personnel to support the national cyberspace strategy.[33] This action should be continued and at the same time, expanded to support student loans for technology degrees focused upon information security. These graduates would then be used to fill the shortages of IT security personnel within the business sector. Also, the government must require that Internet Service Providers (ISP) provide basic security tools and safeguards to its customers. This makes sense for their business interests and strengthens the posture of our national networks. Finally, federal standards, backed by federal incentives, must regulate IT security at the state and local levels. While not politically favorable at first glance, the protection of our information infrastructure is only accomplished as a matter of national defense.

The National Strategy for the Security of Cyberspace establishes the US government as the role model for others to follow; yet it falls short of formally establishing its role of setting standards for IT security. Granted, the establishment of technology standards is a moving target as technology evolves; yet private business, as a group with its shortage of experienced personnel and multiple focuses, has not proven itself dynamic enough to stay abreast of current technology. Therefore, the government is the practical choice to lead a consortium of private and government representatives to establish common standards and best practices for the sound implementation of IT security.

"Red Teams" refer to the government practice of testing its vulnerabilities to cyber attack. Established for federal agencies, these attacks stress and validate an organization's ability to defend its information assets. As the security of our information infrastructure affects all citizens, Red Team actions should be expanded to all sectors of the US portion of the Internet. The program could be phased in as a voluntary assessment of an organization's information security and as the system matures, the Red Team activities could randomly examine business, government and private sector networks by Internet Protocol (IP) domains. As vulnerabilities are determined, Internet service providers (ISP) and IT departments would be notified of their vulnerabilities along with suggested corrections. Red Team activities would soon become analogous to a policeman walking his beat, checking windows and doors for vulnerabilities. With technology advances, many of the Red Team activities can be automated to save costs.

Finally, to avoid the natural resistance to “Big Brother”, Red Team procedures would have to be carefully developed to safeguard individual privacy and property rights.

While falling short of strict government regulation of information security, these forward looking measures provide a variety of incentives and standards to strongly encourage both private and government sectors to strengthen the security of our nation’s cyberspace. The security of our national information infrastructure is critical to the survival and operation of our nation. Fortunately, we have not experienced an information event to match the terrorist attack of September 11th. Yet should we continue with our present policy, we remain vulnerable in this critical infrastructure area. The security of cyberspace serves as an infrastructure protection that enables other national infrastructures. The priority must be placed upon achieving success within this complicated battle space. The US must immediately strengthen its strategy to protect cyberspace and these measures represent the types of action, short of strict regulation, that will improve our ability to preserve our critical resource of functional, trustworthy information infrastructure.

CONCLUSION

The nation continues to experience a phenomenal growth in the Internet accompanied with an exponential increase in our vulnerability of cyber attack. Our daily enemies are becoming more organized and talented, yet experts view the greatest dangers in cyberspace as villains lying in wait: state-sponsored organizations withholding full-fledged cyber attack until the opportunity for sufficient strategic advantage presents itself.[34] Amongst so many potential threats, the United States’ current cyberspace security strategies remain dependent upon voluntary adherence to government recommendations with few regulations, standards or financial incentives to gain private sector or state and local government support.

The United States must reassess its national strategies and with practical incentives, enforce stronger measures to secure its critical information infrastructures. The strategy for reinforcing the security of cyberspace need not be accomplished with heavy-handed regulation. As a balance of responsibility and incentives, the way ahead should embrace the three major areas outlined within this paper. First, on the legal front, companies must clearly recognize their liability for not adhering to recognized best business practices for ensuring the trustworthiness of the development, operation and distribution of information infrastructure related products and services. Along the same vein, the government must update its laws and promote standards of international law commensurate with the severity of cyber crimes. Second, in the role of leadership, the government must serve as both the role model and leader for developing

standards and providing business, academic and tax incentives to strengthen cyber security. Finally, the strategy must expand “red team” activities into the new frontier of probing the national information infrastructure for weakness. Once discovered, these vulnerabilities would be reported to the susceptible organization with recommendations for correction. With a strong proactive strategy, the United States will position itself as the world’s leader in securing cyberspace and serve as an example for other nations to follow.

The United States of America has become thoroughly dependent upon its information infrastructure and supported automated systems. While serving as a prime enabler of the information age, cyberspace also serves as the “perfect environment” where asymmetric foes can strike “indirectly, invisibly, and from their perspective, undetected”.[35] Viewing the threat, the potential losses associated with failure to secure cyberspace are too high. If we continue with partial solutions, the nation will face unforeseen, potentially catastrophic consequences. To maintain a strong information infrastructure during war, peace or national crisis, our national security policy must reflect the incentives and guidelines recommended by this report. Strengthening our national information infrastructure against the hidden enemies of cyberspace is a complex, difficult task, yet with strong direction and partnership across all sectors, the nation can confidently buttress itself against the looming vulnerabilities of an increasingly digital world.

WORD COUNT= 5,237

ENDNOTES

[1] George W. Bush, *The National Strategy to Secure Cyberspace* (Washington, D.C.: The White House, February 2003), p. iii.

[2] James Ellis et al., *Report to the President's Commission on Critical Infrastructure Protection* (Carnegie Mellon University: Pittsburgh, PA, 1997), p. 1.

[3] Internet Software Consortium, "Internet Domain Survey, January 2003," January 2003; available from < http://www.isc.org/ds/WWW-200301/index.html>; Internet; accessed 15 October 2003.

[4] Patrick Allen and Chris Demchak, "The Palestinian-Israeli Cyberwar," *Military Review*, March/April 2003, p. 58.

[5] Ellis et al., p. 5-9.

[6] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared; Terrorist at Threshold of Using Internet as Tool of Bloodshed, Experts Say," *The Washington Post*, 27 June 2002, sec. A, p. 1.

[7] Maroochy Shire Council, "Maroochy Shire Statistics," January 2004; available from <http://www.maroochy.qld.gov.au/fact_file.cfm >; Internet accessed 12 February 2004.

[8] Gellman, p. 1.

[9] Dan Verton, "Offshore Coding Raises Security Concerns," *Computerworld*, 5 May 2003, p. 1-2.

[10] P.J. Anthony, "Adobe to Spend $50 Million to Expand Center in India," *The New York Times*, 25 January 2001, sec. C, p. 1.

[11] Robert B. Reich, "High-Tech Jobs Are Going Abroad! But That's Okay," *The Washington Post*, 2 November 2003, sec. B, p. 3.

[12] Verton, p. 2.

[13] James Brooke, "Japan Braces for a 'Designed in China' World," The New York Times, 21 April 2002, sec. 3, p. 1.

[14] Erik Sherman, "Terror's Next Target; Information Systems That Control Power Plants and Other Critical Facilities are Riddled with Security Holes," *Newsweek* , 22 October 2001, 80.

[15] Robyn Weisman, "California Power Grid Hack Underscores Threat to U.S.," 13 June 2001; available from <http://www.newsfactor.com/perl/story/11220.html>; Internet accessed 16 February 2004.

[16] Clive Thompson, "Digital Doomsday" (Book Review), *The Washington Post*, 10 August 2003, sec. T, p. 4.

[17] Rick White and Stratton Sclavos, "Targeting Our Computers," *The Washington Post*, 15 August 2003, sec. A, p. 27.

[18] Allen, p. 53-55.

[19] James N. Thurman, "The Internet as War's Newest Battlefield," *The Christian Science Monitor*, 9 December 1999, p.1.

[20] Ibid.

[21] United States Department of Justice, "Protecting America's Critical Infrastructure: PDD 63," 8 February 1999; available from <http://www.usdoj.gov/criminal/cybercrime/factsh.htm >; Internet; accessed 26 September 2003.

[22] United States Department of Justice, "CCIPS Critical Infrastructure Protection," 8 February 1999; available from <http://www.usdoj.gov/criminal/cybercrime/critinfr.htm >; Internet; accessed 26 September 2003.

[23] United States Department of Justice, "Protecting America's Critical Infrastructure: PDD 63."

[24] Bush, p. i.

[25] Mark Gibbs, "What the Gov Should Have Done About Security," *Network World*, 30 September 2002, p. 62.

[26] Charles Piller and Jube Shiver JR., "Czar of Cyber Security Defends Easing of Rules," *The Los Angeles Times*, 18 September 2002, sec. A, p. 14.

[27] Gibbs, 62.

[28] Bush, p. 55 – 60.

[29] Daniel Kuehl and Robert E. Neilson, "No Strategy for the Information Age," *Proceedings, United States Naval Institute* , September 2003, 2.

[30] Clint Kreitner, "Encouraging Trends in Information Security," *Infotech Update* , July/August 2003, p. 7.

[31] Piller and Shiver Jr, p. 14.

[32] United States Department of State, International Information Programs, "White House Advisor Richard Clarke Briefs Senate Panel On Cybersecurity," 13 February 2003, available from <http://usinfo.state.gov/topical/pol/terror/02021409.htm >; Internet accessed 16 February 2004.

[33] Ibid.

[34] Dan Kuehl, "Cyberwar's Economic Threat; US is Vulnerable to Foreign Attacks, Hill Panel is Told," *The Washington Post*, 24 February 2000, sec. A, p. 19.

[35] Wayne Hall, *Stray Voltage; War in the Information Age* (Annapolis, MD: Naval Institute Press, 2003), 53.

BIBLIOGRAPHY

Allen, Patrick and Chris Demchak. "The Palestinian-Israeli Cyberwar." *Military Review* (March/April 2003).

Anthony, P.J. "Adobe to Spend $50 Million to Expand Center in India." *The New York Times* (25 January 2001).

Brooke, James. "Japan Braces for a 'Designed in China' World." *The New York Times* (21 April 2002).

Bush, George W. *The National Strategy to Secure Cyberspace.* Washington, D.C.: The White House, February 2003.

Ellis, James, David Fisher, Thomas Longstaff, Linda Pesante, and Richard Pethia. *Report to the President's Commission on Critical Infrastructure Protection*. Pittsburgh, PA : Carnegie Mellon University, 1997.

Gibbs, Mark. "What the Gov Should Have Done About Security." *Network World* (30 September 2002).

Gellman, Barton. "Cyber-Attacks by Al Qaeda Feared; Terrorist at Threshold of Using Internet as Tool of Bloodshed, Experts Say." *The Washington Post* (27 June 2002).

Hall, Wayne. *Stray Voltage; War in the Information Age.* Annapolis, MD: Naval Institute Press, 2003.

Internet Software Consortium. "Internet Domain Survey, January 2003," January 2003. Available from < http://www.isc.org/ds/WWW-200301/index.html>. Internet. Accessed 15 October 2003.

Kreitner, Clint. "Encouraging Trends in Information Security." *Infotech Update* (Vol 12, Issue 4, July/August 2003).

Kuehl, Daniel and Robert E. Neilson. "No Strategy for the Information Age." *Proceedings, United States Naval Institute* (September 2003).

Kuehl, Daniel. "Cyberwar's Economic Threat; US is Vulnerable to Foreign Attacks, Hill Panel is Told." *The Washington Post* (24 February 2000).

Maroochy Shire Council, "Maroochy Shire Statistics," January 2004. Available from <http://www.maroochy.qld.gov.au/fact_file.cfm >. Internet. Accessed 12 February 2004.

Piller, Charles and Jube Shiver JR.. "Czar of Cyber Security Defends Easing of Rules." *The Los Angeles Times* (18 September 2002).

Reich, Robert B. "High-Tech Jobs Are Going Abroad! But That's Okay." *The Washington Post* (2 November 2003).

Sherman, Erik. "Terror's Next Target; Information Systems That Control Power Plants and Other Critical Facilities are Riddled with Security Holes." *Newsweek* (22 October 2001).

Thompson, Clive. "Digital Doomsday" (Book Review). *The Washington Post* (10 August 2003).

Thurman, James N. "The Internet as War's Newest Battlefield." *The Christian Science Monitor* (9 December 1999).

Weisman, Robyn. "California Power Grid Hack Underscores Threat to U.S.," 13 June 2001. Available from <http://www.newsfactor.com/perl/story/11220.html>. Internet. Accessed 16 February 2004.

United States Department of Justice. "CCIPS Critical Infrastructure Protection," 8 February 1999. Available from <http://www.usdoj.gov/criminal/cybercrime/factsh.htm>. Internet. Accessed 26 September 2003.

United States Department of State, International Information Programs. "White House Advisor Richard Clarke Briefs Senate Panel On Cybersecurity," 13 February 2003. Available from <http://usinfo.state.gov/topical/pol/terror/02021409.htm>. Internet accessed 16 February 2004.

United States Department of Justice. "Protecting America's Critical Infrastructure: PDD 63," 8 February 1999. Available from <http://www.usdoj.gov/criminal/cybercrime/factsh.htm>. Internet. Accessed 26 September 2003.

Verton, Dan. "Offshore Coding Raises Security Concerns." *Computerworld* (5 May 2003).

White, Rick and Stratton Sclavos. "Targeting Our Computers." *The Washington Post* (15 August 2003).